ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

A Proposed RSDA Scheme to Defence Attacks in Wireless Ad Hoc Networks

[1]*B Sunil Kumar* [2]*K. Prasad*

[1] *Associate Professor, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.*

[2] *PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.*

Abstract- Performance and Security are two critical functions of Wireless Ad-Hoc Networks (WANETs). Network security ensures the integrity, availability, and performance of WANETs. It helps to prevent critical service interruptions and increases economic productivity by keeping networks functioning properly. Since there is no centralized network management in WANETs, these networks are susceptible to packet drop attacks. In selective drop attack, the neighboring nodes are not loyal in forwarding the messages to the next node. It is critical that the illegitimate node must be identified, which overload the host node and isolate them from the network by holding its transmission process. In this paper, we present a Resistive to Selective Drop Attack (RSDA) scheme to provide effective security against selective drop attack. Alight weight RSDA protocol is proposed for detecting malicious nodes in the network under particular drop attack. The RSDA protocol can be integrated with the many existing routing protocols for WANETs such as AODV and DSR. It accomplishes reliability in routing by disabling the link with the highest weight and authenticate the nodes using the Elliptic Curve Digital Signature Algorithm (ECDSA).

Keywords:Wireless Ad-Hoc Networks, Resistive to Selective Drop Attack (RSDA), Network Security, Elliptic Curve Digital Signature Algorithm (ECDSA).

1. INTRODUCTION

Wireless Ad-Hoc Networks(WANETs) [1] decentralized nature makes suitable for a different type of applications where central nodes cannot be trusted on and may progress the scalability of networks linked to wireless networks, through practical and theoretical confines to the overall size of such networks have been recognized. Minimal configuration and quick deployment make ad hoc networks suitable for emergencies like natural military or disasters conflicts. The existence of adaptive and dynamic routing protocols enables ad hoc networks to be formed quickly. Their applications can further classify wireless Ad-hoc networks. Like Vehicular ad hoc networks (VANETs) [2], Mobile ad hoc networks (MANETs), Smartphone Ad-hoc networks (SPANs) [3], Wireless mesh networks [4] and so on. The packet drop attack [5] can frequently be used to attack WANETs. Wireless networks have much different architecture than that of a typical wired network; a host can broadcast that it has the shortest

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host can drop packets at will [6]. Also, over a mobile ad-hoc network, hosts are especially vulnerable to collaborative attacks where multiple hosts willbecome compromised and deceive the other hosts on the network [7]. The RSDA protocol can provide resistance to selective drop attacks by thwarting the nodes from getting overloaded. It attains reliability in routing using the reliable factor by disabling the link as defective or by obtaining a new efficient route to the destination.

To address the selective drop attack [5], a reliable factor is chosen by computing the list of link weights. If the sum of the weight of a particular route is high, e.g., it indicates that the low reliability [8], the attacking node can be identified. Each node maintains its own weight; the obtained weight is added to the route request payload. By computing the reliability rate,malicious nodes can be distinguished from other normal nodes.

The RSDA protocol has been designed to offer resistance to selective drop attacks by thwarting the nodes from getting overloaded. It attains reliability in routing using the reliable factor by disabling the link as defective or by obtaining a new efficient route to the destination. This paper contributes mainly discussed study on Wireless Ad Hoc Networks and their issues related security perception. A review on various protocols is there to dealing selective drop attack in WANET. A light weight RSDA protocol has been proposing for detecting malicious nodes in the network under selective drop attack. The RSDA protocol can be integrated with the many existing routing protocols for WANET such as AODV and DSR.

An efficient cryptographic technique ECDSA has been chosen for providing authentication which has a lesser key size however it provides similar security. Finally, it achieves extremely Network security ensures the integrity, availability,and performance enhanced using RSDA for WANET.

2. RELATED WORK

In [13] the author, proposed the soft security mechanism as a fully distributed trust-based public key management technique for MANET. Instead of using hard security approaches to eliminate security vulnerabilities, as in the case of traditional security techniques their work aimed at maximizing the performance by relaxing security requirements focusing on the perceived trust. A Composite Trust-based Public Key Management (CTPKM) was proposed to maximize the performance by mitigating the vulnerabilities. A trusted threshold was fixed with each node to decide whether to trust another node or not.

In [14] the author, proposed a security framework named Resilience Evaluation Framework for Ad Hoc routing protocols (REFRAHN)based on the insertion of malicious faults and

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

quantitatively evaluated their effect on routing protocols. The primary goal of REFRAHN is to (i) minimize the uncertainty in the sources while deploying ad hoc routing protocols, (ii) devise fault-tolerant mechanisms that tackle and reduce such problems, and (iii) compare and choose the routing protocol that optimizes the robustness and performance of the network. Methodological aspects regarding fault injection in routing protocols have been extensively analyzed.

In [15] the author, proposed a robust and distributed access control mechanism depending on a trust model for securing the network and encouraging good cooperation by isolating misbehaving nodes in the network. The access control responsibility is viewed in two different contexts namely the local and global. In the local context responsibility, the neighbor nodes are intimated to notify about the suspicious behavior of the global context. While the global context examines the gathered information, a decision would be made to penalize the malicious node using a voting scheme. It was experimentally proven that the combination of voting, trust schemes offered a precise, accurate classification and node exclusion mechanism even in scenarios of limited monitoring.

In [16] the author, described the ad hoc network would function well only if the nodes are trustworthy and good cooperating. A dynamic trust prediction model is presented for evaluating the trustworthiness of nodes depends on nodes historical behavior and future behavior by using extended fuzzy logic rules. Moreover, the proposed trust prediction model is combined into a source route mechanism. The novel technique named Trust-based Source Routing protocol (TSR) [17] offers a flexible, feasible approach for choosing the shortest path by meeting the security requirement of packet transmission. TSR improves packet delivery ratio and reduces average end-to-end latency by conducting more experiments in malicious node detection and attack resistance.

The RSDA protocol has been proposed to offer resistance to selective drop attacks by thwarting the nodes from getting overloaded. It attains reliability in routing by disabling the link as defective or attempts to obtain a new efficient route to the destination. RSDA provides an effective security for selective drop attack. The attacker nodes can potentially drop the throughput of a host to the minimum level, and those nodes have been detected based on ECDSA [11]. The lightweight solution to selective drop attack has been provided by proposing RSDA protocol resists selective drop attacks by preventing the nodes from getting overloaded. Reliability is achieved in routing by rendering the link as defective or attempts to acquire an efficient route to the destination. RSDA assists in maximizing the performance by mitigating the vulnerabilities and defend well in the presence of selective drop attack.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

3. PROPOSED WORK

A) System Model

The figure-1 illustrate the system model for this proposed system as follows

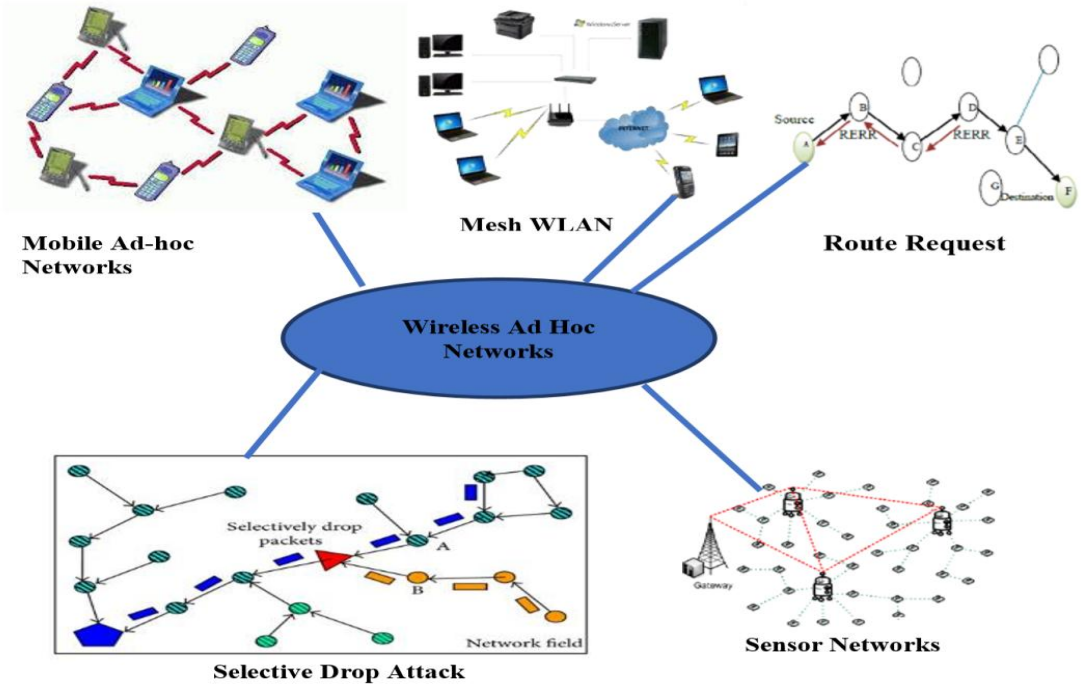


Fig. 1. System Model for Wireless Ad-Hoc Networks (WANETs)

This system model consists and implements the following modules:

Source: In this module, Source browse the file, select the destination and sends to the router. In Source while uploading the file, encrypt and then uploads the file. File content will be initialized to all the nodes.

Router:In this module, router consists of four Networks, each Network contains specific nodes. When Source sends the file initially it comes to the Network1 and passes through the Network1 nodes, if any congestion found in the Network1 node, it automatically selects another node amove to Network2 and Network 3 and Network4 and reaches the destination. The energy size also be modified, view the Network details. In router the routing path and time delay can be viewed.

Router Manager:In this module, Router manager views the attacker details by checking the energy details and find attackers.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

Destination: In this module, Receiver request for file name and secret key and receives the content from the router. Time delay will be calculated by sending the file from source to destination and time taken to reach the destination.

Attacker: In this module, attacker selects the Network and node, gets the original energy size and modifies the energy size for the node.

B) Methodology

Node detection: Failure of anode would have an impact on the routing packets. Hence, such type of nodes should be detected and isolated to avoid network partitioning, which inturn affect the survival of the network. The failed node can typically be detected using routing protocols.

Node isolation: The cases have been described for node isolation by considering the following scenarios,

Effect of failed and selfish node: If the node n3is a failed node and if a node s starts a route discovery process to node d, the failed node n3cannot forward the packets received from the downstream nodes. If neighbors of node s are failed, then s would be unable to communicate with other nodes. Hence, the node s is said to be isolated by all its neighbors. If the node n3 is taken as a selfish node as shown in figure2, when node s starts a route discovery process to node d, the selfish node n3 may be reluctant to forward the request from s. In this case, n3 behaves like a failed node. The node n3 may discard data packets and forwards only control packets which are forwarded to it. Thus, the communication [10] between s and d would not be ensured. If the neighbors of s are selfish, s would not be capable of communicating with other nodes, which are at one hop distance. Although the selfish nodes can still communicate with the remaining nodes, it is distinguished from the failed node.

C) Algorithms

Algorithm 1: Key generation.

1. Begin
2. Generate Random Number (nonce) k.
3. Form Private Key d.
4. Compute e = HASH(m), // HASH is cryptographic hash function.
5. Let z be the Lnleftmost bits of e, where Ln is the bit length of the group order n.
6. Choice a Cryptographically Secure Random (CSR) integer k from [1, n-1].
7. Compute the curve point (x, y) = k×G.

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

8. Compute r = x mod n If r=0, go back to step 3.
9. Compute s = k−1(z = rdA) mod n. If s=0, go to step Select CSR.
10. signature is the pair (r,s).
11. Finally, form a Public Key Q (x, y)
12. End

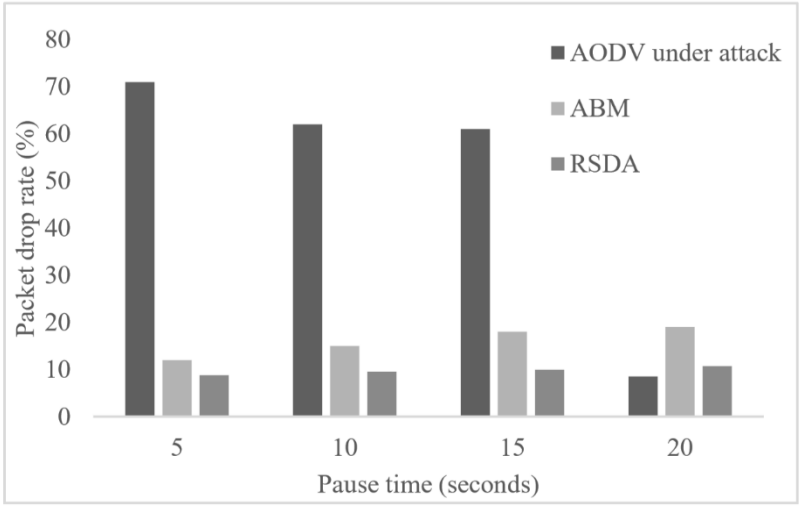
Algorithm 2: Signature verification

1. Begin
2. Created message can be sent Y for verification using authenticator's public key
3. The message digest is intended with the public key q (x, y)
4. Digital signature elements r and s
5. Check that Qx is not equal to the identity element O, and its coordinates are otherwise valid
6. Y to authenticate X signature
7. Check that Qx lies on the curve
8. X can verify $Qx$is a valid curve point for successfully sending
9. All verification elements with domain Parameters (p, n, a, b, x, y)
10. Check that $n \times Qx = O$
11. Consecutive secure Public key with different curve points
12. End

4. RESULTS AND DISCUSSION

In this section, we provide the proposed scheme comparative analysis results.The simulation has been conducted to validate the detection and isolation of the proposed scheme against gray hole nodes.

Packet Drop Rate:



ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

Fig. 2. Packet drop rate vs. pause time

The drop ratewas raised to about 63.9% when there were gray hole nodes randomly fixed at various positions at all pause time as 5, 10, 15,20seconds respectively. In the presence of gray hole nodes, the total packet drops rate of ABMachieved was16.7%. With the deployment of proposed RSDA, the drop rate successfully reduced to about 9.56% rate, as shown in figure 2. The packet drop rate is shown to decrease significantly when more misbehaving nodes make abnormal routing operations. This effect is particularly severe to the network with more number of nodes.

Routing Overhead:

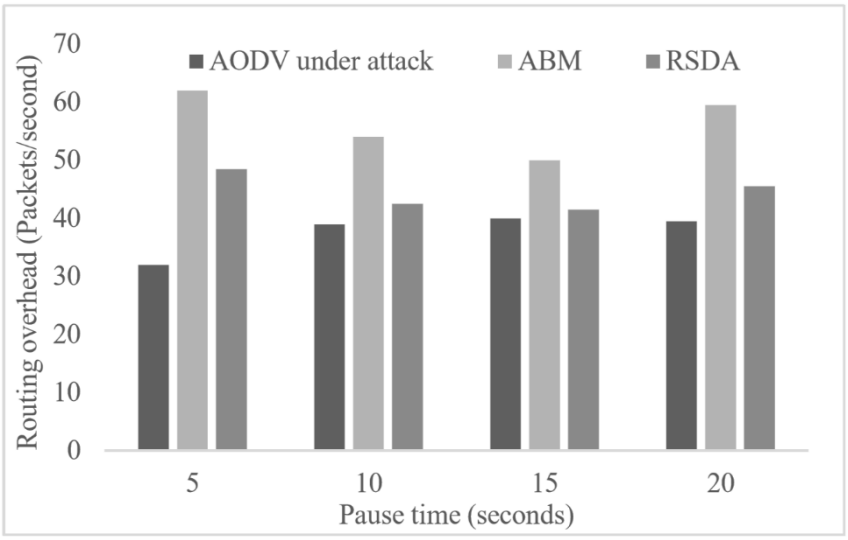


Fig. 3. Routing overhead vs. pause time

The routing overhead was raised to about 77.84% when there are gray hole nodes were randomly fixed at various positions at all pause time as 5s, 10s, 15s, 20seconds respectively. In the presence of gray hole nodes, the routing overhead of ABM was56.85%. With the deployment of proposed RSDA, the routing overhead was successfully reduced to about 45.49% rate, as shown in figure 3.

Packet Drop Rate for Randomly Moved Gray Hole Nodes:

In addition to 60 normal nodes distributed, 1 or 2 gray hole nodes in network topology are considered separately. First, it was assumed that gray hole nodes are randomly moved. The

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

total packet drop rate of one gray hole node and two gray hole nodes are as shown in Figures 4 and 5 respectively.

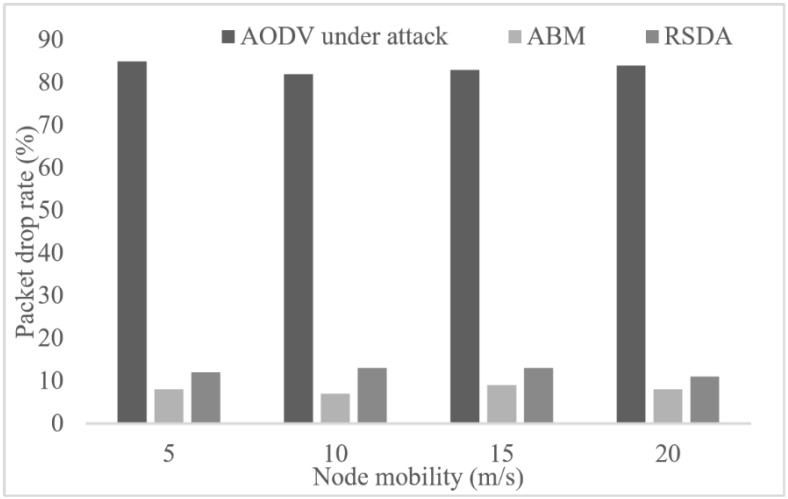


Fig. 4. One gray hole nodes for node mobility vs. packet drop rate

In the absence of gray hole nodes, the total packet drop rate for all mobility speed by AODV is about 7.93% with all nodes randomly moved. The drop rate raises to about 86.75% when there is one gray hole node randomly fixed at various positions. With the deployment of proposed RSDA, the drop rate can successfully reduce by about 12.63%. In the absence of two gray hole nodes, the total packet drop rate for all mobility speed by AODV is about 8.6% with all nodes randomly moved.

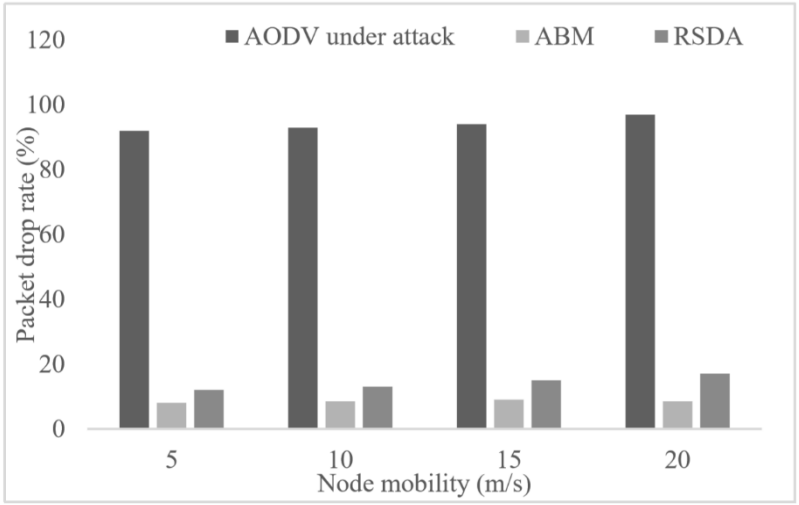


Fig. 5. Two gray holes nodes for node mobility vs. packet drop rate

The drop rate is raised to about 94.89% when there are two grey hole nodes randomly fixed at various positions. With the deployment of the proposed RSDA, the drop rate can successfully have reduced by about 14.5%. An interesting observation is that the proposed method shortens the packet drop rate significantly, especially for the scalable network. In fact, the

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

decrease in packet drop rate is since it achieves the significant security level with less key size.

5. CONCLUSION

Resistive to Selective Drop Attack (RSDA) attempts to provide an effective security for selective drop attack. It is important that the illegitimate nodes should be identified which overload a host and isolate them from thenetwork by holding its transmission process. In selective drop attack, the neighboring nodes will not loyally forward their messages to the next node. However, a malicious node which has been entered itself in the data flow path can deny specific forwarding messages. The malicious nodes have to be detected, which is overloading a host and entirely stop it from working. Thus, the node which denies forwarding certain messages, but sending other messages acted unpredictably. In selective drop attack, the malicious nodes would be refusing of forwarding messages passing through them. At last the attack can potentially drop the throughput of a host to the minimum level. Security in a WANET environment requires a precise point of view, from which security can be provided by mitigating the protection against various types of attacks.

REFERENCES

1. Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, “Wireless ad hoc networks,” Encycl. Telecommun., 2002.
2. S. Yousefi, M. S. Mousavi, and M. Fathy, “Vehicular ad hoc networks (VANETs): challenges and perspectives,” in ITS Telecommunications Proceedings, 2006 6th International Conference on, 2006, pp. 761– 766.
3. H. Deng, W. Li, and D. P. Agrawal, “Routing security in wireless ad hoc networks,” IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75, 2002.
4. I. F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: a survey,” Comput. networks, vol. 47, no. 4, pp. 445–487, 2005.
5. V. Balakrishnan and V. Varadharajan, “Packet drop attack: A serious threat to operational mobile ad hoc networks,” in Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi, 2005, pp. 89–95.
6. M. Peng, W. Shi, J.-P. Corriveau, R. Pazzi, and Y. Wang, “Black hole search in computer networks: State-of-the-art, challenges and future directions,” J. Parallel Distrib. Comput., vol. 88, pp. 1–15, 2016.

7. Rajasekar, P. and Mangalam, D. (2016) Efficient FPGA implementation of AES 128 bit for IEEE 802.16e mobile WiMax standards. Circuits and Systems, 7, 371-380. doi: 10.4236/cs.2016.74032.
8. J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, and C.-F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," IEEE Syst. J., vol. 9, no. 1, pp. 65–75, 2015.
9. A. Aijaz and A. H. Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective," IEEE Internet Things J., vol. 2, no. 2, pp. 103–112, 2015.
10. P. Chen, S. Cheng, and K. Chen, "Information Fusion to Defend Intentional Attack in Internet of Things," IEEE Internet Things J., vol. 1, no. 4, pp. 337–348, 2014.
11. X. Meng and T. Chen, "Event-driven communication for sampled-data control systems," Am. Control Conf. (ACC), 2013, no. 1, pp. 3002– 3007, 2013.
12. F. Razzak, "Spamming the Internet of Things: A possibility and its probable solution," Procedia Comput. Sci., vol. 10, pp. 658–665, 2012.
13. Viswanth, V. S, Ramanujam, R, and Rajyalakshmi, G. "Performance study of eco-friendly dielectric in EDM of AISI 2507 super duplex steel using Taguchi-fuzzy TOPSIS approach". International Journal of Productivity and Quality Management, vol. 29, No. 4, pp. 518-541, 2020.
14. J.-H. Cho, R. Chen, and K. S. Chan, "Trust threshold based public key management in mobile ad hoc networks," Ad Hoc Networks, vol. 44, pp. 58–75, 2016.
15. J. Friginal, D. de Andrés, J.-C. Ruiz, and M. Martínez, "REFRAHN: a resilience evaluation framework for ad hoc routing protocols," Comput. Networks, vol. 82, pp. 114–134, 2015.
16. L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An accurate and precise malicious node exclusion mechanism for ad hoc networks," Ad hoc networks, vol. 19, pp. 142–155, 2014.
17. H. Xia, Z. Jia, X. Li, L. Ju, and E. H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," Ad Hoc Networks, vol. 11, no. 7, pp. 2096–2114, 2013.

Author's Profile:

Mr. B Sunil Kumar has received his M.Sc Computer Science from SVU PG Center, Kavali affiliated to Sri Venkateswara University in 2002, M.Tech degree in Information

ISSN: 2278-4632
Vol-10 Issue-6 No. 7 June 2020

Technology from Sathyabama University, Chennai in 2009 and M.Tech in Computer Science and Engineering from SVCET, Chittoor affiliated to JNTU, Anantapur in 2013. He is pursuing Ph.D in CSE at SVU, Uttar Pradesh. He is dedicated to teaching field from the last 14 years. He has guided 26 P.G and 40 U.G students. His research areas included Data Mining. At present he is working as Assistant Professor in Narayana Engineering College, Gudur, Andhra Pradesh, India.

K. Prasadhas received his B.Sc degree in Computer Science from Kakatheeya Degree College, Podalakur affiliated to VikramaSimhapuri University, Nellore in 2017 and pursuing PG degree in Mater of Computer Applications (MCA) from Narayana Engineering College, Gudur affiliated to JNTU, Ananthapur, AndhraPradesh, India.

